BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
Brittany S. Scott (State Bar No. 327132)
Joshua R. Wilner (State Bar No. 353949)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
Email: ltfisher@bursor.com
bscott@bursor.com
jwilner@bursor.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ELIA RAMIREZ, individually and on behalf of all others similarly situated,

Plaintiff,

v.

TRUSPER, INC. d/b/a MUSELY,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Elia Ramirez ("Plaintiff") brings this action on behalf of herself and all others similarly situated against Trusper, Inc. ("Defendant" or "Musely"). Plaintiff brings this action based upon personal knowledge of the facts pertaining to herself, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

NATURE OF THE ACTION

1. This is a class action lawsuit brought on behalf of all U.S. residents who have accessed and used www.musely.com (the "Website"), a website Defendant owns and operates.

2. Defendant aids employs, agrees, and conspires with Meta[1] to intercept communications sent and received by Plaintiff and Class Members, including communications containing protected medical information. Plaintiff brings this action for legal and equitable remedies resulting from these illegal actions.

PARTIES

Defendant

3. Defendant Trusper, Inc. is a Delaware Corporation with its principal place of business at 3300 Central Expressway, Suite C Santa Clara, CA 95051. Defendant does business under the name Musely and owns and operates the Website.

Plaintiff

4. Plaintiff Elia Ramirez is a natural person and citizen of California, residing in Riverside, California.

5. In or around August 2023, Plaintiff Ramirez visited the Website. While navigating the Website, she searched for and purchased a treatment for dark brown spots on the skin. As part of the purchase process, as is the case with all purchases on the Website, Plaintiff answered a series of questions related to the condition of her skin for the purpose of having a doctor write a prescription for the medication she purchased with the understanding that the medication would not be shipped to her without the doctor giving her a prescription.

[1] In October 2021, Facebook, Inc. changed its name to Meta Platforms, Inc. Unless otherwise indicated, Facebook, Inc. and Meta Platforms, Inc. are referenced collectively as "Meta."

6. Plaintiff Ramirez has had an active Facebook account for several years. Plaintiff routinely accesses Facebook on her computer using her Google Chrome browser.

7. Pursuant to the systematic process described herein, Defendant assisted Meta with intercepting Plaintiff Ramirez's communications, including those that contained personally identifiable information ("PII"), protected health information ("PHI"), and related confidential information. Defendant assisted these interceptions without Plaintiff Ramirez's knowledge, consent, or express written authorization.

8. After placing her order from the Musely Website, Plaintiff began receiving targeted advertisements from Musely and other advertisements related to prescription skincare on Facebook.

9. By failing to receive the requisite consent, Defendant breached its duties of confidentiality and unlawfully disclosed Plaintiff Ramirez's personally identifiable information and protected health information.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000, exclusive of interest and costs, and at least one member of the proposed class is a citizen of a state different from at least one Defendant.

11. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is in this District.

12. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because Defendant resides in this District.

FACTUAL ALLEGATIONS

A. Background of the California Information Privacy Act ("CIPA")

13. The CIPA, Cal. Penal Code § 630, *et seq.*, prohibits aiding or permitting another person to willfully—and without the consent of all parties to a communication—read or learn the contents or meaning of any message, report, or communication while the same is in transit or

passing over any wire, line, or cable, or is being sent from or received at any place within California.

14. To establish liability under Cal. Penal Code § 631(a), a plaintiff need only establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following:

> Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,
>
> Or
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,
>
> Or
>
> Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

15. Section 631(a)'s applicability is not limited to phone lines, but also applies to "new technologies" such as computers, the internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' internet browsing history).

16. Under Cal. Penal Code § 637.2, Plaintiff and Class Members may seek injunctive relief and statutory damages of $5,000 per violation.

B. Background of the California Confidentiality of Medical Information Act ("CMIA")

17. Pursuant to the California Confidentiality of Medical Information Act ("CMIA"), a "provider of health care . . . shall not disclose medical information regarding a patient of the provider of health care . . . without first obtaining an authorization, except as provided in subdivision (b) or (c)." Cal Civ. Code § 56.10(a). "An authorization for the release of medical information . . . shall be valid if it:

> (a) Is handwritten by the person who signs it or is in a typeface no smaller than 14-point type.
>
> (b) Is clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization.
>
> (c) Is signed and dated . . .
>
> (d) States the specific uses and limitations on the types of medical information to be disclosed.
>
> (e) States the name or functions of the provider of health care, health care service plan, pharmaceutical company, or contractor that may disclose the medical information.
>
> (f) States the name or functions of the persons or entities authorized to receive the medical information.
>
> (g) States the specific uses and limitations on the use of the medical information by the persons or entities authorized to receive the medical information.
>
> (h) States a specific date after which the provider of health care, health care service plan, pharmaceutical company, or contractor is no longer authorized to disclose the medical information.
>
> (i) Advises the person signing the authorization of the right to receive a copy of the authorization."

Cal. Civ. Code § 56.11.

18. Moreover, a health care provider that maintains information for purposes covered by the CMIA is liable for negligent disclosures that arise as the result of an affirmative act—such as implementing a system that records and discloses online patients' personally identifiable

information and protected health information. Cal. Civ. Code § 56.36(c). Similarly, if a negligent release occurs and medical information concerning a patient is improperly viewed or otherwise accessed, the individual need not suffer actual damages. Cal. Civ. Code § 56.36(b).

19. "In addition to any other remedies available at law, any individual may bring an action against any person or entity who has negligently released confidential information or records concerning him or her in violation of this part, for either or both of the following: [¶] (1) ... nominal damages of one thousand dollars ($1,000). In order to recover under this paragraph, it shall not be necessary that the plaintiff suffered or was threatened with actual damages. [¶] (2) The amount of actual damages, if any, sustained by the patient." *Sutter Health v. Superior Ct.*, 227 Cal. App. 4th 1546, 1551, 174 Cal. Rptr. 3d 653, 656 (2014) (quoting Cal. Civ. Code § 56.36(b)).

C. Defendant's Website

20. Defendant specializes in selling "custom prescription skincare" treatments.[2]

21. Throughout its Website and marketing, Defendant emphasizes that it is a provider of medical services, that "offer[s] prescriptions; not products."[3]

22. In order to obtain the prescription medication sold on Defendant's Website, patients complete a questionnaire related to the condition of their skin. After the order is placed, a doctor reviews the responses to the questionnaire and writes a prescription for a particular treatment, prompting the shipment of the treatment product. Through the Musely app, patients continue to check in with an "eNurse" after their purchase to continue to receive effective treatment.[4]

23. Defendant's Website is accessible on mobile devices and desktop computers. Defendant also offers the Musely app available for download on Android and iPhone devices.

[2] About Musely https://www.musely.com/facerxstory (Last accessed March 21, 2024).
[3] *Id.*
[4] *Id.*

D. Meta's Platform and its Business Tools

24. Facebook, owned by Meta, describes itself as a "real identity platform,"[5] meaning users are allowed only one account and must share "the name they go by in everyday life."[6] To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.[7]

25. In 2021, Meta generated over $117 billion in revenue.[8] With respect to the apps offered by Meta, substantially all of Meta's revenue is generated by selling advertising space.[9]

26. Meta sells advertising space by highlighting its ability to target users.[10] Meta can target users so effectively because it surveils user activity both on and off its sites.[11] This allows Meta to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[12] Meta compiles this information into a generalized dataset called "Core Audiences," which allows advertisers to reach precise audiences based on specified targeting types.[13]

27. Advertisers can also build "Custom Audiences."[14] Custom Audiences enables advertisers to reach "people who have already shown interest in [their] business, whether they're

---

[5] Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021).

[6] FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity.

[7] FACEBOOK, SIGN UP, https://www.facebook.com.

[8] FACEBOOK, META ANNUAL REPORT 2021, https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/2023/2021-Annual-Report.pdf at 51.

[9] *Id.* at 63.

[10] FACEBOOK, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES, https://www.facebook.com/business/help/205029060038706.

[11] FACEBOOK, ABOUT META PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

[12] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.

[13] https://www.facebook.com/business/news/Core-Audiences.

[14] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494.

loyal customers or people who have used [their] app or visited [their] website."[15] With Custom Audiences, advertisers can target existing customers directly, and they can also build "Lookalike Audiences," which "leverage[] information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[16] Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Meta with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers or by utilizing Meta's "Business Tools."[17]

28. As Meta puts it, the Business Tools "help website owners and publishers, app developers, and business partners, including advertisers and others, integrate with [Facebook], understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[18] Put more succinctly, Meta's Business Tools are bits of code that advertisers can integrate into their websites, mobile applications, and servers, thereby enabling Meta to intercept and collect user activity on those platforms.

29. The Business Tools are automatically configured to capture certain data, like when a user visits a webpage, that webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase.[19] Meta's Business Tools can also track other events. Meta offers a menu of "standard events" from which advertisers can choose,

---

[15] FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.

[16] FACEBOOK, ABOUT LOOKALIKE AUDIENCES, https://www.facebook.com/business/help/164749007013531?id=401668390442328.

[17] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; FACEBOOK, CREATE A WEBSITE CUSTOM AUDIENCE, https://www.facebook.com/business/help/1474662202748341?id=2469097953376494.

[18] FACEBOOK, THE META BUSINESS TOOLS, https://www.facebook.com/help/331509497253087.

[19] *See* FACEBOOK, META FOR DEVELOPERS: META PIXEL, ADVANCED, https://developers.facebook.com/docs/meta-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR META PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, META FOR DEVELOPERS: MARKETING API - APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

including what content a visitor views or purchases.[20] Advertisers can even create their own tracking parameters by building a "custom event."[21]

30. One such Business Tool is the Facebook Pixel (the "Facebook Pixel"). Meta offers this piece of code to advertisers, like Defendant, to integrate into their websites. The Facebook Pixel "tracks the people and type of actions they take."[22] When a user accesses a website hosting the Facebook Pixel, Meta's software script surreptitiously directs the user's browser to contemporaneously send a separate message to Meta's servers. This secret and contemporaneous transmission contains the original GET request sent to the host website, along with additional data that the Facebook Pixel is configured to collect. This transmission is initiated by Meta code and concurrent with the communications with the host website. At relevant times, two sets of code were thus automatically run as part of the browser's attempt to load and read Defendant's Website—Defendant's own code and Facebook's embedded code.

31. Defendant chose to include the Facebook Pixel on its Website.

32. Meta's own documentation makes clear just how much tracking of private information the Facebook Pixel does. It describes the Facebook Pixel as code that Meta's business customers can put on their website to "[m]ake sure your ads are shown to the right people. ***Find … people who have visited a specific page or taken a desired action on your website***." (Emphasis added.)[23]

33. Meta instructs such business customers that:

> Once you've set up the [Facebook] Pixel, ***the pixel will log when someone takes an action on your website***. Examples of actions include adding an item to their shopping cart or making a purchase. ***The Pixel receives these actions, or events***,

[20] FACEBOOK, SPECIFICATIONS FOR META PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142.

[21] FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, META FOR DEVELOPERS: MARKETING API – APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[22] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting.

[23] Meta, ABOUT META PIXEL https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Dec. 26, 2023).

> which you can view on your [Facebook] Pixel page in Events Manager. From there, you'll be able to see the actions that your customers take. ***You'll also have options to reach those customers again through future Meta ads***.[24]

34. Of course, in healthcare, it is medical specialists and healthcare treatments that users "add to their shopping cart." They make doctor's appointments rather than making purchases.

35. The Facebook Pixel code enables Meta not only to help Defendant with advertising to its own patients outside the Website, but also to include individual patients among groups targeted by ***other*** Facebook advertisers relating to the conditions about which patients communicated on Defendant's Website.

36. Meta's Business Help Center explains:

> Meta ***uses marketing data to show ads to people who are likely to be interested in them***. One type of marketing data is website events, which are ***actions that people take on your website***.[25]

37. In other words, Meta sells advertising space by highlighting its ability to target users.[26] Meta can target users so effectively because it surveils user activity both on and off its sites, including Facebook.[27] This allows Meta to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and connections.[28]

38. An example illustrates how the Facebook Pixel works. Take an individual who, at relevant times, navigated to Defendant's Website and clicked on a link for information about dark spot treatments. When that link was clicked, the individual's browser sent a GET request to Defendant's server requesting that server to load the particular webpage. As a result of Defendant's use of the Facebook Pixel, Meta's embedded code, written in JavaScript, sent secret

---

[24] *Id*. (Emphasis added.)

[25] Meta, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS https://www.facebook.com/business/help/964258670337005?id=1205376682832142 (emphasis added)

[26] Meta, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES, https://www.facebook.com/business/help/205029060038706 (last visited Dec. 26, 2023).

[27] Meta, ABOUT META PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142

[28] Meta, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting

instructions back to the individual's browser, without alerting the individual that this was happening. Meta caused the browser to secretly duplicate the communication with Defendant, transmitting it to Meta's servers, alongside additional information that transcribed the communication's content and the individual's identity.

39. After collecting and intercepting the information described in the preceding paragraph, Meta processed it, analyzed it, and assimilated it into datasets like Core Audiences and Custom Audiences.

E. How Defendant Disclosed Plaintiff's and Class Members' Protected Health Information and Assisted with Intercepting Communications

40. Through the Facebook Pixel, Defendant shared its patients' identities and online activity, including information and search results related to their private medical treatment.

41. Each time Defendant sent this activity data, it also disclosed a patient's personally identifiable information, including their Facebook ID ("FID"). An FID is a unique and persistent identifier that Facebook assigns to each user. With it, any ordinary person can look up the user's Facebook profile and name. Notably, while Meta can easily identify any individual on its Facebook platform with only their unique FID, so too can any ordinary person who comes into possession of an FID. Meta admits as much on its website. Indeed, ordinary persons who come into possession of the FID can connect to any Facebook profile.

42. A user who accessed Defendant's Website while logged into Facebook transmitted what is known as a "c_user cookie" to Facebook, which contained that user's unencrypted Facebook ID.

43. When a visitor's browser had recently logged out of an account, Facebook compelled the visitor's browser to send a smaller set of cookies.

44. One such cookie was the "fr cookie" which contained, at least, an encrypted Facebook ID and browser identifier. [29] Facebook, at a minimum, used the fr cookie to identify users. [30]

45. If a visitor had never created an account, an even smaller set of cookies was transmitted.

46. At each stage, Defendant also utilized the "_fbp cookie," which attached to a browser as a first-party cookie, and which Facebook used to identify a browser and a user. [31]

47. The c_user cookie expires after 90 days if the user checked the "keep me logged in" checkbox on the website.[32] Otherwise, the c_user cookie is cleared when the browser exits.[33]

48. The The fr cookie expires after 90 days unless the visitor's browser logs back into Facebook.[34] If that happens, the time resets, and another 90 days begins to accrue.[35]

49. The _fbp cookie expires after 90 days unless the visitor's browser accesses the same website.[36] If that happens, the time resets, and another 90 days begins to accrue.[37]

50. The Facebook Pixel used both first- and third-party cookies. A first-party cookie is "created by the website the user is visiting"—*i.e.*, Defendant's Website.[38] A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—*i.e.*,

---

[29] DATA PROTECTION COMMISSIONER, FACEBOOK IRELAND LTD, REPORT OF RE-AUDIT (Sept. 21, 2012), http://www.europe-v-facebook.org/ODPC_Review.pdf.

[30] FACEBOOK, PRIVACY CENTER – COOKIES POLICY, https://www.facebook.com/privacy/policies/cookies/?subpage=subpage-1.3.

[31] *Id.*

[32] Seralthan, FACEBOOK COOKIES ANALYSIS (Mar. 14, 2019), https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbdf8a.

[33] *Id.*

[34] *See id.*

[35] Confirmable through developer tools.

[36] FACEBOOK, PRIVACY CENTER – COOKIES POLICY, https://www.facebook.com/privacy/policies/cookies/?subpage=subpage-1.3.

[37] Also confirmable through developer tools.

[38] PC MAG, FIRST-PARTY COOKIE, https://www.pcmag.com/encyclopedia/term/first-party-cookie. This is confirmable by using developer tools to inspect a website's cookies and track network activity.

Facebook.[39] The _fbp cookie was always transmitted as a first-party cookie. A duplicate _fbp cookie was sometimes sent as a third-party cookie, depending on whether the browser had recently logged into Facebook.

51. Meta at a minimum, used the fr, _fbp, and c_user cookies to link to Facebook IDs and corresponding Facebook profiles. Defendant sent these identifiers alongside the event data.

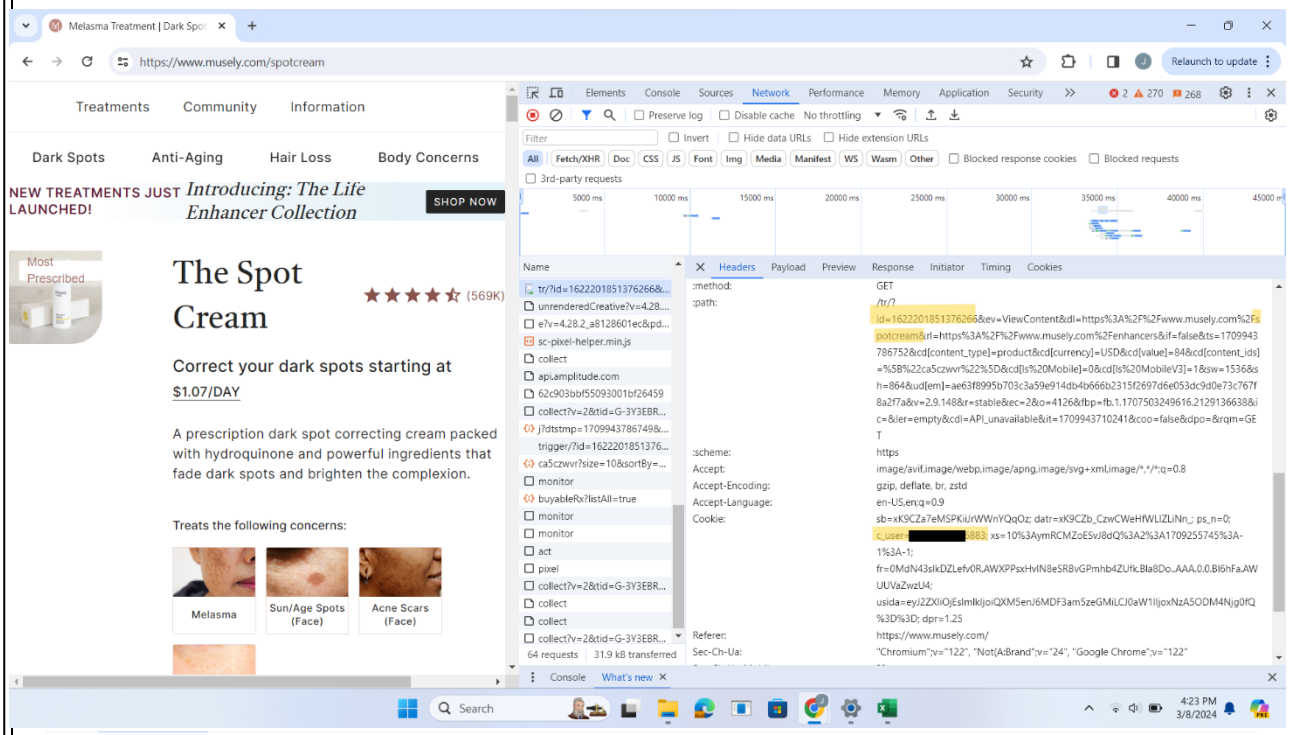
52. What is more, when a user checks out on Musely.com Meta is sent the email address used to check out. The email address is encrypted by way of a process known as SHA256, which is a way to "hash" written words in a series of random numbers.

53. The Meta Pixel is designed to collect information about website visitors that can be matched to an individual's Facebook profile for the purpose of sending targeted advertising to that user. Though the "hashing" would prevent a party that is not Meta from obtaining the subscriber's email address, Meta, as the recipient of the data and the entity that creates the hash, can decrypt the hashed email addresses it receives and match it to the profile of Facebook users.

54. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendant to disclose her personally identifiable information and protected health information. Plaintiff was never provided with any written notice that Defendant disclosed the protected health information of users of the Website, nor was she provided any means of opting out of such disclosures. Defendant nonetheless knowingly disclosed Plaintiff's protected health information to Facebook.

55. When a Musely patient visits the page for a dark spot treatment, the treatment purchased by Plaintiff, Meta deploys the Facebook Pixel with a pixel ID number of 1622201851376266, and automatically receives the page URL, which discloses the treatment sought, and the patient's Facebook ID via the c_user cookie.

[39] PC MAG, THIRD-PARTY COOKIE, https://www.pcmag.com/encyclopedia/term/third-party-cookie. This is also confirmable by tracking network activity.



56. Further, when a patient "checks out" (completes a purchase) the Facebook Pixel, deployed with the same pixel ID number, receives another event, this time showing that an item

was purchased from Musely and receiving a hashed version of the email entered during check out (identified by the ud[em] marking).

Facebook
id 1622201851376266
ev SubscribedButtonClick
dl https://www.musely.com/facerx/checkout
rl https://www.musely.com/facerx/loginstatus
if false
ts 1710773531464
cd[buttonFeatures] {"classList":"var-button__content","destination":"","id":"","imageUrl":"","innerText":"PLACE ORDER","numChildButtons":0,"tag":"div","type":null}
cd[buttonText] PLACE ORDER
cd[formFeatures] []
cd[pageFeatures] {"title":"Prescription Skincare That Works | Musely FaceRx"}
sw 1920
sh 1080
ud[em] 2a9a22d88b031064ea86ff104d1cabf6b14a866c2a4adf136def1330b49fecbb
udff[em] 6139e8a0a7389590e6c239c6c7aa163aadb77e0732b891df718958d90b901d2f
udff[zp] ebc2c8afb60ce18c389cd7b4ce7abdd1d2ad14559f360a36740689fe861b5d26
v 2.9.150
r stable
ec 30
o 7198
fbp fb.1.1710772832874.918794581
ic fbpixel
ler empty
cdl API_unavailable
it 1710772965966
coo false
dpo
es automatic
tm 3
rqm GET

57. By law, Plaintiff is entitled to privacy in her protected health information and confidential communications. Defendant deprived Plaintiff of her privacy rights when it: (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online patients' confidential communications, personally identifiable information, and protected health information; (2) disclosed patients' protected health information to Meta—an unauthorized

third-party eavesdropper; and (3) undertook this pattern of conduct without notifying Plaintiff and without obtaining her express written consent. Plaintiff did not discover that Defendant disclosed her personally identifiable information and protected health information to Meta, and assisted Meta with intercepting her communications, until March 2024.

F. Federal Warning on Tracking Codes on Healthcare Websites

58. The government has issued guidance warning that tracking code like the Facebook Pixel may violate federal privacy law when installed on healthcare websites. The statement titled, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates (the "Bulletin"), was issued by the Department of Health and Human Services' Office for Civil Rights ("OCR") in December 2022.[40]

59. Healthcare organizations regulated under the Health Insurance Portability and Accountability Act (HIPAA) may use third-party tracking tools, such as the Facebook Pixel, in a limited way, to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' PHI to these vendors. The Bulletin explains:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[41]

60. The bulletin discusses the types of harm that disclosure may cause to the patient:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule[fn] but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, ***discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI***. Such disclosures can reveal incredibly sensitive information about an individual, ***including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment***. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, ***because of the proliferation of tracking technologies collecting sensitive information, now more***

[40] HHS.gov, USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

[41] *Id.* (Emphasis added.)

> ***than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.***[42]

61. Plaintiff and the Class face just the risks about which the government expresses concern. Defendant disclosed Plaintiff's and Class Members' search terms about health conditions for which they seek doctors; their contacting of doctors to make appointments; the frequency with which they take steps relating to obtaining healthcare for certain conditions; and where they seek medical treatment. This information is, as described by the OCR in its bulletin, "highly sensitive."

62. The Bulletin goes on to make clear how broad the government's view of protected information is. It explains:

> This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, ***or any unique identifying code***.[43]

63. Crucially, that paragraph in the government's Bulletin continues:

> ***All such [individually identifiable health information ("IIHI")] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.*** This is because, ***when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care***.[44]

64. Then, in July 2022, the Federal Trade Commission ("FTC") and the Department of Health and Human Services ("HHS") issued a joint press release warning healthcare providers about the privacy and security risks arising from the use of online tracking technologies:

> The Federal Trade Commission and the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) are cautioning [healthcare providers] and telehealth providers about the privacy and security risks related to the use of online tracking technologies integrated into their websites or mobile apps that may be impermissibly disclosing consumers' sensitive personal health data to third parties.
>
> "When consumers visit a [healthcare provider's] website or seek telehealth services, they should not have to worry that their most private and sensitive health

---

42 *Id.* (Emphasis added.)

43 *Id*. (Emphasis added.)

44 *Id*. (Emphasis added.)

> information may be disclosed to advertisers and other unnamed, hidden third parties," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers' health information from potential misuse and exploitation."
>
> "Although online tracking technologies can be used for beneficial purposes, patients and others should not have to sacrifice the privacy of their health information when using a [healthcare provider's] website," said Melanie Fontes Rainer, OCR Director. "OCR continues to be concerned about impermissible disclosures of health information to third parties and will use all of its resources to address this issue."
>
> The two agencies sent the joint letter to approximately 130 [healthcare providers] and telehealth providers to alert them about the risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies gather identifiable information about users, usually without their knowledge and in ways that are hard for users to avoid, as users interact with a website or mobile app.
>
> In their letter, both agencies reiterated the risks posed by the unauthorized disclosure of an individual's personal health information to third parties. For example, the disclosure of such information could reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, and where an individual seeks medical treatment.
>
> . . . Through its recent enforcement actions against BetterHelp, GoodRx and Premom, as well as recent guidance from the FTC's Office of Technology, the FTC has put companies on notice that they must monitor the flow of health information to third parties that use tracking technologies integrated into websites and apps. The unauthorized disclosure of such information may violate the FTC Act and could constitute a breach of security under the FTC's Health Breach Notification Rule. . . .[45]
> Therefore, Defendant's conduct is directly contrary to clear pronouncements by the FTC and HHS.

65. In light of, and in addition to, the government's own issued guidance above, news sources are also warning that tracking code, like the Facebook Pixel, poses risks of violating federal privacy law and HIPAA:

[45] Federal Trade Commission, *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies*, July 20, 2023, https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking.

> Federal regulators are warning [healthcare providers] and telehealth providers about the data privacy risks of using third-party tracking technologies.
>
> These services, like [Facebook Tracking] Pixel or Google Analytics, could violate the Health Insurance Portability and Accountability Act (HIPAA) or Federal Trade Commission (FTC) data security rules, officials said.
>
> The FTC and the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) issued a rare joint release announcing that 130 [healthcare providers] and telehealth providers received a letter warning them about the data privacy and security risks related to the use of online tracking technologies integrated into their websites or mobile apps.... "The compliance buck still stops with you. Furthermore, your company is legally responsible even if you don't use the data obtained through tracking technologies for marketing purposes."[46]

Fierce Healthcare also spoke up in an April 3, 2023 article:

> Nearly all nonfederal acute care [healthcare providers'] websites track and transfer data to a third party, potentially fueling the unwanted disclosures of patients' sensitive health information and opening up that [healthcare provider] to legal liability, according to a recently published University of Pennsylvania analysis. [https://www.healthaffairs.org/doi/full/10.1377/hlthaff.2022.01205]. The census of more than 3,700 [healthcare provider] homepages found at least one third-party data transfer among 98.6% of the websites as well as at least one third-party cookie on 94.3%, researchers wrote in Health Affairs.
>
> The [healthcare providers'] homepages had a median of 16 third-party transfers… Many of these complaints cite Facebook parent company Meta's Pixel tracker, which a June 2022 investigation from The Markup [https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites] detected on about a third of [health care providers'] websites. That report found evidence that, in some instances, the sensitive data transferred to third parties met the criteria for a HIPAA violation.[47]

Health Affairs also published an article in April 2023, stating:

> By including third-party tracking code on their websites, [healthcare providers] are facilitating the profiling of their patients by third parties. These practices can lead to dignitary harms, which occur when third parties gain access to sensitive health information that a person would not wish to share. These practices may also lead

[46] Heather Landi, *Regulators warn hospitals and telehealth companies about privacy risks of Meta, Google tracking tech*, FIERCE HEALTHCARE, July 21, 2023, https://www.fiercehealthcare.com/health-tech/regulators-warn-hospitals-and-telehealth-companies-about-privacy-risks-meta-google

[47] Dave Muoio, *Almost every hospital's homepage is sending visitors' data to third parties, study finds*, FIERCE HEALTHCARE, Apr. 3, 2023, https://www.fiercehealthcare.com/providers/almost-every-hospital-homepage-sending-visitors-data-third-parties-study-finds

> to increased health-related advertising that targets patients, as well as to legal liability for [healthcare providers].[48]

66. On July 20, 2023, the OCR and FTC sent Defendant, through its CEO, Jack Jia, a letter to draw Defendant's attention to "serious privacy and security risks related to the use of online tracking technologies that may be present on [its] website or mobile application (app) and ***impermissibly disclosing consumers' sensitive personal health information to third parties***." (Emphasis Added) A true and correct copy of the warning letter is attached hereto as **Exhibit A**. The letter went on to emphasize the serious nature of such disclosures:

> Impermissible disclosures of an individual's personal health information to third parties may result in a wide range of harms to an individual or others. Such disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more. In addition, impermissible disclosures of personal health information may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others.

Id.

67. On March 18, 2024. HHS published a revised version of the bulletin, which further clarified that "identifying information showing [a patient's] visit to [a public] webpage is a disclosure of PHI to the extent that the information is both identifiable and related to the individual's health or future health care."[49]

68. This is further evidence that the data that Defendant chose to share is protected Personal Information. The sharing of that information was a violation of Class Members' rights.

CLASS ALLEGATIONS

69. Class Definition: Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of herself and other similarly situated individuals defined as

[48] Ari B. Friedman, et al., *Widespread Third-Party Tracking On Hospital Websites Poses Privacy Risks For Patients And Legal Liability For Hospitals*, HEALTH AFFAIRS, Vol. 42, No. 24, April 2023, https://www.healthaffairs.org/doi/10.1377/hlthaff.2022.01205

[49] *HHS.gov, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.*

all persons in the United States who, during the class period, had their personally identifiable information or protected health information improperly disclosed to Meta and other third party entities, as a result of using the Website (the "Class" or "Nationwide Class").

70. Plaintiff also seeks to represent a subclass consisting of Class members who, during the class period, had their personally identifiable information or protected health information improperly disclosed to Meta and other third party entities, as a result of using the Website while located in California (the "California Subclass" or "Subclass").

71. Plaintiff reserves the right to modify the class definition or add sub-classes as necessary prior to filing a motion for class certification.

72. The "Class Period" is the time period beginning on the date established by the Court's determination of any applicable statute of limitations, after considering of any tolling, concealment, and accrual issues, and ending on the date of entry of judgement.

73. Excluded from the Class and Subclass is Defendant; any affiliate, parent, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer director, or employee of Defendant; any successor or assign of Defendant; anyone employed by counsel in this action; any judge to whom this case is assigned, his or her spouse and immediate family members; and members of the judge's staff.

74. Numerosity/Ascertainability. Members of the Class and Subclass are so numerous that joinder of all members would be unfeasible and not practicable. The exact number of Class and Subclass Members is unknown to Plaintiff at this time; however, it is estimated that there are thousands of individuals in the Class and Subclass. The identity of such membership is readily ascertainable from Musely's records and non-party records, such as those of Meta.

75. Typicality. Plaintiff's claims are typical of the claims of the Class and Subclass because Plaintiff used the Website and, as a result of Defendant's unlawful conduct, had her PII and PHI intercepted by third parties, such as Meta, without her express written authorization or knowledge. Plaintiff's claims are based on the same legal theories as the claims of other Class and Subclass Members.

76. Adequacy. Plaintiff is fully prepared to take all necessary steps to represent fairly and adequately the interests of the Class and Subclass Members. Plaintiff's interests are coincident with, and not antagonistic to, those of the members of the Class and Subclass. Plaintiff is represented by attorneys with experience in the prosecution of class action litigation generally and in the emerging field of digital privacy litigation specifically. Plaintiff's attorneys are committed to vigorously prosecuting this action on behalf of the members of the Class and Subclass.

77. Common Questions of Law and Fact Predominate/Well Defined Community of Interest. Questions of law and fact common to the members of the Class and Subclass predominate over questions that may affect only individual members of the Class and Subclass because Defendant has acted on grounds generally applicable to the Class and Subclass. Such generally applicable conduct is inherent in Defendant's wrongful conduct. Questions of law and fact common to the Classes include:

(a) Whether Defendant intentionally tapped the lines of internet communication between patients and their medical provider;

(b) Whether Musely's Website contains code that permits third parties, such as Meta, to intercept patients' personally identifiable information, protected health information, and related communications;

(c) Whether Meta is a third-party eavesdropper;

(d) Whether Plaintiff's and Class Members' communications via the Website and the resultant interceptions thereof constitute an affirmative act of communication;

(e) Whether Musely's conduct, which allowed Meta and other entities—unauthorized persons—to view Plaintiff's and Class Members' personally identifiable information and PHI, resulted in a breach of confidentiality;

(f) Whether Defendant violated Plaintiff's, Class, and Subclass Members' privacy rights by using third-party technology, such as the Facebook Pixel, to allow third parties to intercept patients' online communications along with information that uniquely identified the patients;

(g) Whether Plaintiff, Class, and Subclass Members are entitled to damages under CIPA, the CMIA, or any other relevant statute; and

(h) Whether Defendant's actions violate Plaintiff's, Class, and Subclass Members' privacy rights as provided by the California Constitution.

78. Superiority. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweighs potential difficulties in management of this class action. Plaintiff knows of no special difficulty to be encountered in litigating this action that would preclude its maintenance as a class action.

COUNT I
Violation of the California Invasion of Privacy Act
Cal. Penal Code § 631

79. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the members of the Class and Subclass.

80. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. CIPA begins with its statement of purpose – namely, that the purpose of CIPA is to "protect the right of privacy of the people of [California]" from the threat posed by "advances in science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications . . . ." Cal. Penal Code § 630.

81. A person violates California Penal Code § 631(a), if:

> by means of any machine, instrument, or contrivance, or in any other manner, [s/he] intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or [s/he] willfully and without the consent of all

> parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or [s/he] uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained . . . .

Cal. Penal Code § 631(a).

82. Further, a person violates § 631(a) if s/he "aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned" in the preceding paragraph. *Id.*

83. To avoid liability under § 631(a), a defendant must show it had the consent of all parties to a communication.

84. At all relevant times, Defendant aided, agreed with, and conspired with Meta to track and intercept Plaintiff's and Class Members' internet communications while accessing www.memorialcare.org. These communications were intercepted without the authorization and consent of Plaintiff and Class Members.

85. Defendant, when aiding and assisting Meta's wiretapping, intended to help Meta learn some meaning of the content in the URLs and the content the visitor requested.

86. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, the Facebook Pixel falls under the broad catch-all category of "any other manner":

a. The computer codes and programs Meta used to track Plaintiff's and Class Members' communications while they were navigating musely.com;

b. Plaintiff's and Class Members' browsers;

c. Plaintiff's and Class Members' computing and mobile devices;

d. Meta's web and ad servers;

e. The web and ad-servers from which Meta tracked and intercepted Plaintiff's and Class Members' communications while they were using a web browser to access or navigate musely.com;

f. The computer codes and programs used by Meta to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a browser to visit musely.com; and

g. The plan Meta carried out to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser or mobile application to visit musely.com.

87. The patient communication information that Defendant transmitted using the Facebook Pixel, such as information regarding prescription dermatology treatment, constituted protected health information.

88. As demonstrated hereinabove, Defendant violated CIPA by aiding and permitting third parties to receive its patients' online communications through the Website without their consent.

89. As a result of the above violations, Defendant is liable to Plaintiff and other Class Members in the amount of, the greater of, $5,000 dollars per violation or three times the amount of actual damages. Additionally, Cal. Penal Code § 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages."

90. Under the statute, Defendant is also liable for reasonable attorney's fees, and other litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Defendant in the future.

COUNT II
Violation of the California Confidentiality of Medical Information Act
Cal. Civ. Code § 56.10

91. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the members of the Class and Subclass.

92. Under the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56.10 ("CMIA"), providers of health care are prohibited from disclosing medical information relating to their patients without a patient's authorization. Medical information refers to "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care . . . regarding a patient's medical history, mental or physical condition, or treatment. "Individually Identifiable" means that the medical information includes or

contains any element of personal identifying information sufficient to allow identification of the individual . . . ."

93. Musely is a "provider of healthcare" under the CMIA because it (1) employs board-certified dermatologists to review patient's conditions and write prescriptions for its products (Cal. Civ. Code §56.05(p)) and because it maintains medical information and offers software to consumers that is designed to maintain medical information for the purpose of allowing its users to manage their information or make the information available to a healthcare provider, or for the diagnosis, treatment, or management of a medical condition (Cal. Civ. Code §56.06(a)-(b)).

94. Plaintiff and Class Members are patients, and, as a health care provider, Defendant had an ongoing obligation to comply with the CMIA's requirements.

95. As set forth hereinabove, a Facebook ID is an identifier sufficient to allow identification of an individual. Along with patients' Facebook ID and email address, Defendant disclosed to Meta several pieces of information regarding its patients' use of Defendant's Website, which, on information and belief, included, but was not limited to: patient medical conditions, medical concerns, treatment patients were seeking, and the fact that patients were seeking a prescription for treatment of those conditions.

96. This patient information was derived from a provider of health care regarding patients' medical treatment and physical condition. Accordingly, it constituted medical information pursuant to the CMIA.

97. As demonstrated hereinabove, Defendant failed to obtain its patients' valid authorization for the disclosure of medical information.

98. Pursuant to CMIA § 56.11, a valid authorization for disclosure of medical information must: (1) be "[c]learly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization"; (2) be signed and dated by the patient or her representative; (3) state the name and function of the third party that receives the information; and (4) state a specific date after which the authorization expires. Accordingly, information set forth in Defendant's Website Privacy Policy does not qualify as a valid authorization.

99. Based on the above, Defendant violated the CMIA by disclosing its patients' medical information to Meta along with the patients' Facebook IDs and email addresses.

100. Under the CMIA, a patient may recover compensatory damages, punitive damages not to exceed $3,000 dollars and attorneys' fees not to exceed $1,000, and the costs of litigation for any violating disclosure of medical information. Alternatively, a patient may recover nominal damages of $1,000 for any negligent release of medical information.

COUNT III
Invasion of Privacy Under California's Constitution

101. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the members of the Class and Subclass.

102. Plaintiff and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential communications and protected health information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to wiretaps without Plaintiff's and Class Members' knowledge or consent.

103. At all relevant times, by using the Facebook Pixel to record and communicate patients' Facebook IDs alongside their confidential medical communications, Defendant intentionally invaded Plaintiff's and Class Members' privacy rights under the California Constitution.

104. Plaintiff and Class Members had a reasonable expectation that their communications, identities, health information, and other data would remain confidential, and that Defendant would not install wiretaps on www.musely.com.

105. Plaintiff and Class Members did not authorize Defendant to record and transmit Plaintiff's and Class Members' private medical communications alongside their personally identifiable health information.

106. This invasion of privacy was serious in nature, scope, and impact because it related to patients' private medical communications. Moreover, it constituted an egregious breach of the societal norms underlying the privacy right.

107. Accordingly, Plaintiff and Class Members seek all relief available for invasion of privacy claims under California's Constitution.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an order certifying the Class and the Subclass under Rule 23 of the Federal Rules of Civil Procedure, naming Plaintiff as the representative of the Class and Subclass, and Plaintiff's attorneys as Class Counsel to represent the Class and Subclass members.

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct alleged in this Complaint pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;

C. For an order finding in favor of Plaintiff, the Class, and the Subclass on all counts asserted herein;

D. For an award of damages, including, but not limited to, actual, consequential, statutory, punitive, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: April 2, 2024

BURSOR & FISHER, P.A.

By: */s/ Brittany S. Scott*
Brittany S. Scott

L. Timothy Fisher (State Bar No. 191626)
Brittany S. Scott (State Bar No. 327132)
Joshua R. Wilner (State Bar No. 353949)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
Email: ltfisher@bursor.com
bscott@bursor.com
jwilner@bursor.com

Attorneys for Plaintiff

EXHIBIT A

July 20, 2023

Musely
3300 Central Expressway, Suite C
Santa Clara, CA 95051
Attn: Jack Jia, CEO

Re: Use of Online Tracking Technologies

Dear Mr. Jia,

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) are writing to draw your attention to serious privacy and security risks related to the use of online tracking technologies that may be present on your website or mobile application (app) and impermissibly disclosing consumers' sensitive personal health information to third parties.

Recent research,[1] news reports,[2] FTC enforcement actions,[3] and an OCR bulletin[4] have highlighted risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies

---

[1] *See, e.g.,* Mingjia Huo, Maxwell Bland, and Kirill Levchenko, *All Eyes on Me: Inside Third Party Trackers' Exfiltration of PHI from Healthcare Providers' Online Systems*, Proceedings of the 21st Workshop on Privacy in the Electronic Society (Nov. 7, 2022), https://dl.acm.org/doi/10.1145/3559613.3563190.

[2] *See, e.g.,* Todd Feathers, Katie Palmer, and Simon Fondrie-Teitler, *Out of Control: Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, THE MARKUP (Dec. 13, 2022), https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies.

[3] *U.S. v. Easy Healthcare Corp.*, Case No. 1:23-cv-3107 (N.D. Ill. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v; *In the Matter of BetterHelp, Inc.*, FTC Dkt. No. C-4796 (July 14, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter; *U.S. v. GoodRx Holdings, Inc.*, Case No. 23-cv-460 (N.D. Cal. 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc; *In the Matter of Flo Health Inc.*, FTC Dkt. No. C-4747 (June 22, 2021), https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc.

[4] U.S. Dept. of Health and Human Svcs. Office for Civil Rights, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

gather identifiable information about users as they interact with a website or mobile app, often in ways which are not avoidable by and largely unknown to users.

Impermissible disclosures of an individual's personal health information to third parties may result in a wide range of harms to an individual or others. Such disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more. In addition, impermissible disclosures of personal health information may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

If you are a covered entity or business associate ("regulated entities") under HIPAA, you must comply with the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules), with regard to protected health information (PHI) that is transmitted or maintained in electronic or any other form or medium.

The HIPAA Rules apply when the information that a regulated entity collects through tracking technologies or discloses to third parties (*e.g.,* tracking technology vendors) includes PHI. HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or any other violations of the HIPAA Rules. OCR's December 2022 bulletin about the use of online tracking technologies by HIPAA regulated entities provides a general overview of how the HIPAA Rules apply.[5] This bulletin discusses what tracking technologies are and reminds regulated entities of their obligations to comply with the HIPAA Rules when using tracking technologies.

FTC Act and FTC Health Breach Notification Rule

Even if you are not covered by HIPAA, you still have an obligation to protect against impermissible disclosures of personal health information under the FTC Act and the FTC Health Breach Notification Rule. This is true even if you relied upon a third party to develop your website or mobile app and even if you do not use the information obtained through use of a tracking technology for any marketing purposes. As recent FTC enforcement actions demonstrate, it is essential to monitor data flows of health information to third parties via technologies you have integrated into your website or app.[6] The disclosure of such information without a consumer's authorization can, in some circumstances, violate the FTC Act as well as constitute a breach of security under the FTC's Health Breach Notification Rule.[7] Within the last

[5] *Id.*
[6] *See supra* note 3.
[7] *See* Federal Trade Comm'n, *Statement of the Commission on Breaches by Health Apps and Other Connected Devices* (Sept. 15, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.

few months, the FTC has issued a series of guidance pieces addressed to entities collecting, using, or disclosing sensitive health information.[8]

OCR and the FTC remain committed to ensuring that consumers' health privacy remains protected with respect to this critical issue. Both agencies are closely watching developments in this area. To the extent you are using the tracking technologies described in this letter on your website or app, we strongly encourage you to review the laws cited in this letter and take actions to protect the privacy and security of individuals' health information.[9]

Sincerely,

(b)(6)

Melanie Fontes Rainer
Director
Office for Civil Rights
U.S. Department of Health and Human Services

(b)(6)

Samuel Levine
Director
Bureau of Consumer Protection
Federal Trade Commission

---

[8] *See, e.g.*, FTC Office of Technology, *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking* (Mar. 16, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking; Lesley Fair, *First FTC Health Breach Notification Rule case addresses GoodRx's not-so-good privacy practices* (Feb. 1, 2023), https://www.ftc.gov/business-guidance/blog/2023/02/first-ftc-health-breach-notification-rule-case-addresses-goodrxs-not-so-good-privacy-practices; Federal Trade Comm'n and the U.S. Department of Health & Human Services' Office of the National Coordinator for Health Information Technology (ONC), Office for Civil Rights (OCR), and Food and Drug Administration (FDA), *Mobile Health App Interactive Tool* (Dec. 2022), https://www.ftc.gov/business-guidance/resources/mobile-health-apps-interactive-tool; Kristin Cohen, *Location, health, and other sensitive information: FTC Committed to fully enforcing the law against illegal use and sharing of highly sensitive data* (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal.

[9] In addition to the HIPAA Rules, the FTC Act, and the FTC Health Breach Notification Rule, you may also be subject to other state or federal statutes that prohibit the disclosure of personal health information.